志翔科技
ZSHIELD INC

移动内网安全解决方案

场景及案例

针对政府、科技、教育、电力等行业中移动内网作业需求和移动办公需求（双域双系统终端），本方案提供网络安全、终端基础安全和数据安全等三道安全防线，从而使得终端得到管控，数据得到有效保护；本方案已在国家电网某省电力公司移动办公安全加固项目中得到了应用。

方案价值

- 有效减少移动终端被感染和被攻击的机会
- 阻止在移动终端工作区安装和运行非法APP
- 防止因移动终端被劫持或丢失等原因造成的数据和文件泄露

方案亮点

- 构建全面的安全移动作业和移动办公环境
- 利用安全探针技术构建可信计算环境
- 围绕核心数据和应用程序的监控报警系统
- 基于大数据分析与风险预警的安全可视化
- 采用MDM安全策略控制工作区安全权限

通过移动内网安全解决方案，员工能够安全使用优质移动内网业务应用，如相关移动作业、OA、内网邮箱、协同办公等。该解决方案以安全终端为核心，构建了体系化的移动端整体安全架构。其通过“可信计算”、“终端安全”、“系统安全”、“应用安全”、“数据安全”、“接入安全”等全方位的安全防护策略构建了一个可信的、高质量的移动内网安全环境。

针对同一移动终端需访问内外网的场景，采用“双系统”终端实现内外网访问切换，杜绝外网对内网安全的影响；同时在内网系统实施该方案，保证内网安全。

关于志翔科技

志翔科技是国内创新型的大数据安全企业，致力于为政企客户提供核心数据保护和业务风险管控两个方向的产品及服务。志翔科技打破传统固定访问边界，以数据为新的安全中心，为企业构筑兼具事前感知、发现，事中阻断，事后溯源，并不断分析与迭代的安全闭环，解决云计算时代的“大安全”挑战。志翔科技是2017年IDC中国大数据安全创新者，2018年安全牛中国网络安全50强企业。2019年，志翔云安全产品入选Gartner《云工作负载保护平台市场指南》。

更多信息

如欲了解有关志翔科技至安盾®ZS-ISP、至明®ZS-ISA安全探针产品的更多信息，请联系您的志翔科技销售代表，或访问官方网站：www.zshield.net

扫码关注志翔

北京志翔科技股份有限公司
www.zshield.net

电话：010-82319123
邮箱：sales@zshield.net

北京市海淀区学院路35号世宁大厦1101
邮编：100191

业务痛点

移动终端被攻击

使用单系统终端时，若终端从内网到外网来回切换，将极大增加终端被感染和攻击的机会。

移动终端被劫持或丢失

由于员工的疏忽，导致移动终端被劫持或丢失，造成核心数据和机密文件的泄露。

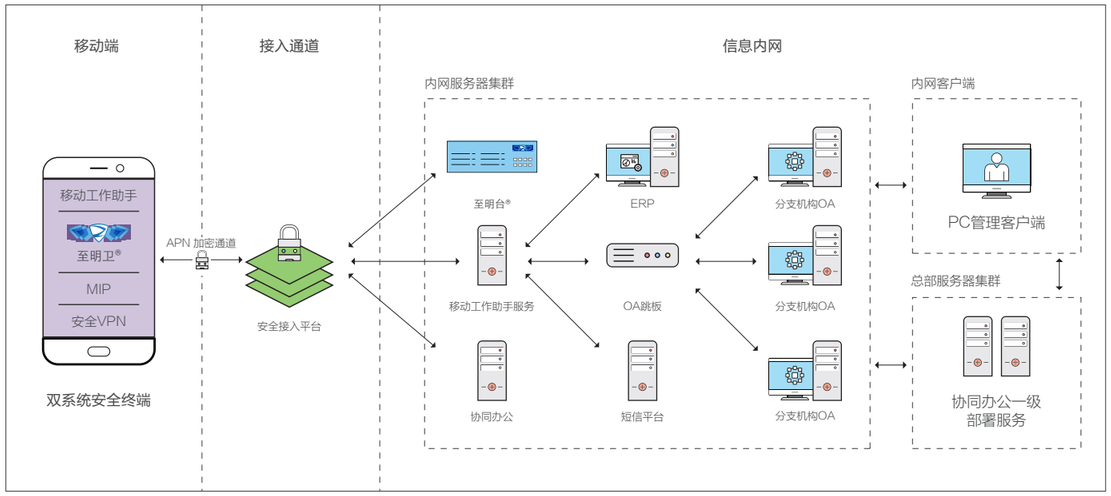
IO端口被非法访问

移动终端工作区的运行环境中没有设置安全策略控制工作区本地的IO权限，本地USB、蓝牙、WiFi和存储卡等会轻易被非法访问。

非法APP被安装

移动终端没有设置安全管控策略，例如白名单机制，可以任意安装非法APP，并用来访问重要数据，从而造成泄密。

解决方案



解决方案示意图（以移动办公为例）

移动终端

终端：(双系统)安全手机终端；
SIM卡：采用移动运营商的SIM卡，可绑定单位专属APN；
安全TF卡（Trans-flash Card）：采用安全TF卡作为安全根证书。

接入通道

可采用单位在运营商的专属通道；
VPN：采用VPN进行传输过程中的数据加密和通道加密。

接入平台

通过安全接入平台进行终端认证和接入的校验；
通过MIP实现统一的账户/密码（统一权限）登录。

至明卫®安全探针和至明台®安全策略平台

构建可信计算环境，通过设置应用程序“白名单”等方式，保证设备运行时的数据和网络安全；

威胁分析与防护能力保证篡改的业务客户端软件无法通过认证检测，从而无法访问业务数据；

利用大数据分析技术，对安全事件进行预警，同时对安全事件进行记录，便于追溯；

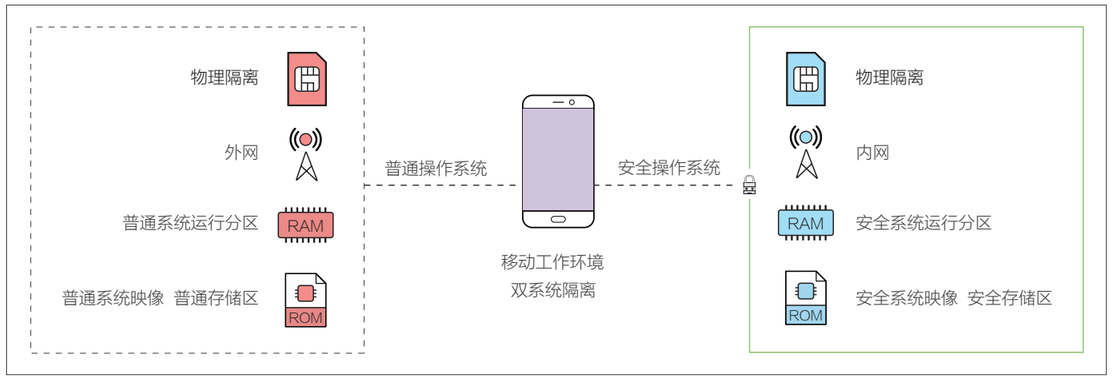
当探测到移动终端丢失或者被劫持时，可强制清除终端上的数据，防止数据泄露。

功能优势

网络环境安全

工作环境：设备的工作环境永远在“干净”的内网，极大减少了被感染和攻击的机会。

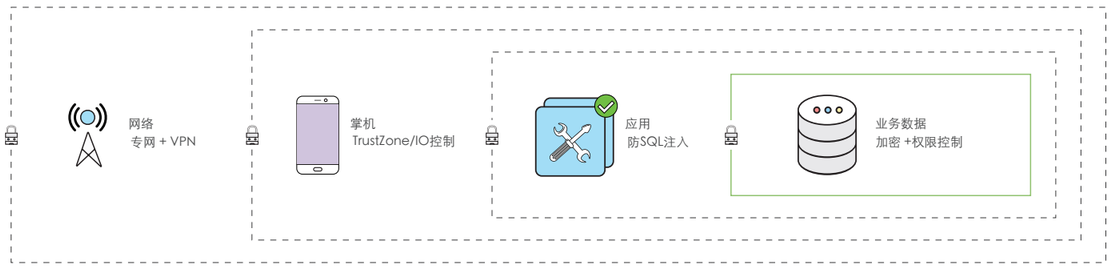
操作系统：可在同一个终端上运行两套Android操作系统，实现内网访问和外网访问的安全隔离。



基础设施安全

信道：通过VPN进行信道加密，保证接入安全。
掌机：工作区基于TrustZone构建，工作区只能访问内网。
工作区：双系统终端中，应用运行环境与私人区完全隔离。

应用：防止SQL注入，并通过白名单机制保证应用安全。
数据：保证本地存储的业务数据是加密的，通过配置权限来控制对服务器上数据的访问。



应用数据安全

可信计算：保证只有认证过的应用才能访问数据及网络。
记录行为：记录应用行为及数据访问行为。

风险预警：基于大数据分析，风险行为会及时预警。
事件追溯：对任何安全事件，都可以追根溯源。